REMARKS

The Examiner has rejected Claims 1-47 under 35 U.S.C. 102(e) as being anticipated by Douik, et al. (U.S. Patent No. 6,012,152). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on the following excerpts from Douik to make a prior art showing of applicant's claimed "filtering a set of intrusion rules to create a subset of rules corresponding to the active networked application" (see this or similar, but not identical language in each of the independent claims).

> "The overall process involves filtering and correlation of alarms, and performing diagnostic tests and performance measures." (Col. 3, lines 20-22-emphasis added)
>
> "The model analyzer sub-agent 34 performs two main functions: rule generation and rule interpreting. Rule generation consists of taking the rules as written for the functional blocks (which refer to internal states, operational states, and intermediate states) and utilizing the connectivity information (signal transmission) to generate rules that explicitly refer to adjacent functional blocks." (Col. 23, lines 57-63-emphasis added)
>
> "Knowledge model Based Reasoning differs from Rule Based Reasoning, where rules contain shallow expert knowledge. Model Based Reasoning can be either based on a model of the "working" system or the "not working" system. In this case, both the "working" and the "not working" system are modeled by a set of production rules. A detected symptom is matched against these production rules in order to find the possible faults." (Col. 20, lines 15-22)
>
> "Knowledge Acquisition and Representation
>
> The SFM system 10 of the present invention utilizes integrated intelligent agents to support users in acquiring and representing mobile telecomunications network knowledge." (Col. 20, lines 63-67)

Applicant respectfully asserts that such excerpts merely teaches "filtering...of alarms" (emphasis added). Clearly, filtering alarms, as in Douik, does not meet

applicant's claimed "filtering a set of intrusion rules" (emphasis added). In addition, nowhere in Douik is there any disclosure of filtering to "create a subset of rules," as claimed by applicant (emphasis added). Instead, Douik only discloses "rule generation and rule interpreting" (see emphasized excerpt above).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Douik reference, as noted above. Thus, a notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the Douik reference, as follows:

> "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application, where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and
>
> evaluating network traffic using the subset of intrusion rules;
>
> wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources" (see this or similar, but not identical language in each of the independent claims).

Applicant respectfully asserts that simply nowhere in the Douik reference is there any disclosure of intrusion rules or a subset of intrusion rules, as argued by applicant with respect to the independent claims. Furthermore, Douik does not teach that the "intrusion rules...are capable of being used for evaluating intrusions that target the corresponding active networked application," or that they are used "for reducing a required amount of processing resources," in the specific manners claimed by applicant. Only applicant teaches and claims such filtering to create an intrusion rule subset capable of being used for evaluating intrusions that target a corresponding active networked application, for the specific purpose of reducing a required amount of processing resources, in the particular context claimed.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 2 et al., the Examiner has relied on Col. 37, lines 5-18 from Douik to make a prior art showing of applicant's claimed "detecting when the active networked application becomes inactive; and re-filtering the set of intrusion rules." However, applicant notes that such excerpt merely teaches determining "whether a successful diagnosis was obtained" and analyzing a "relationship between the involved components." Clearly, such teachings fail to meet applicant's specific claim language, namely "detecting when the active networked application becomes inactive" and "re-filtering the set of intrusion rules" (emphasis added).

Also, with respect to Claim 4 et al., the Examiner has relied on Col. 35, lines 53-55 from Douik to make a prior art showing of applicant's claimed "monitoring application terminations." Applicant respectfully asserts that such excerpt simply teaches "the scheduling of [the] measurement program" which includes termination. Clearly, scheduling a termination of a program does not meet applicant's claimed "monitoring application terminations."

With respect to Claim 5 et al., the Examiner has relied on Col. 9, lines 25-30 and Col. 10, lines 8-9 from Douik to make a prior art showing of applicant's claimed

"detecting when no networked application is active; and suspending the evaluating of network traffic until a networked application is active." Applicant respectfully asserts that such excerpts only teach an "expert system...[that] receives network performance data...recognizes and interprets anomalies, plans solutions, and...installs appropriate controls and monitors" and troubleshooting when a "fault has caused an error or a failure in the system" (emphasis added). However, such excerpts do not teach "detecting when no network application is active" or even "suspending the evaluating of network traffic until a networked application is active," as specifically claimed by applicant (emphasis added).

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 48-51 below, which are added for full consideration:

"wherein the intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol" (see Claim 48);

"wherein the intrusion rules include an attack signature" (see Claim 49);

"wherein at least one of the intrusion rules is a heuristic rule" (see Claim 50); and

"wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made" (see Claim 51).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P345/01.239.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100